

СХВАЛЕНО

педагогічною радою ЗДО № 217

Протокол № 1 від 28.08.2025



ЗАТВЕРДЖЕНО

Директор ЗДО № 217

Лариса ЯЦЕНКО

ПОЛОЖЕННЯ
про цифрову безпеку
закладу дошкільної освіти (ясел-садка)
комбінованого типу № 217 «Грайлик» Запорізької міської ради

I РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу дошкільної освіти (ясел-садка) комбінованого типу № 217 «Грайлик» ЗМР» визначає політику цифрової безпеки закладу дошкільної освіти (ясел-садка) № 217 «Грайлик» ЗМР (далі – ЗДО № 217).

Положення «Про цифрову безпеку закладу дошкільної освіти (ясел-садка) комбінованого типу № 217 «Грайлик» ЗМР» (далі – Положення) описує основні принципи побудови системи управління інформаційною безпекою закладу дошкільної освіти, посадових обов'язків і практик, які використовуються закладом дошкільної освіти для зменшення цифрових ризиків та збереження персональних даних учасників освітнього процесу.

Положення розроблене з урахуванням вимог законів України «Про освіту», «Про повну загальну середню освіту», «Про дошкільну освіту», «Про позашкільну освіту»; законів України, дія яких поширюється на впровадження та використання інформаційних технологій у сфері освіти в Україні: «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні комунікації», «Про основні засади забезпечення кібербезпеки України», «Про електронні документи та електронний документообіг».

У Положення нижченаведені терміни вживаються в такому значенні:

база персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

безпека мережі - здатність електронних комунікаційних мереж протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж, а також даних, що зберігаються, передаються чи обробляються;

гаджет – пристрій, пристосування, яке виконує обмежене коло завдань;

дані - інформація, яка подана у формі, придатній для її оброблення електронними засобами;

документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

девайс – пристрій, пристосування, створене людиною для вирішення широкого кола завдань, комп'ютерна техніка та електроніка;

електронні інформаційні ресурси - систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або програмних продуктів;

засоби інформатизації - комп'ютери, програмні продукти, інформаційні системи або їх окремі елементи, електронні комунікаційні мережі, що використовуються для реалізації інформаційно-комунікаційних технологій;

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформатизація - сукупність взаємопов'язаних організаційних, правових, технологічних, виробничих інших процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій;

інформаційно-комунікаційні технології - результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг;

інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

інформаційна діяльність - це створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації;

комунікація - це процес спілкування і передачі інформації між людьми або їх групами у вигляді усних і письмових повідомлень;

месенджер – телекомунікаційна служба для обміну текстовими повідомленнями між комп'ютерами або іншими пристроями користувачів через комп'ютерні мережі;

мобільний пристрій – це загальний термін для будь-якого портативного комп'ютера або смартфон;

оцифрування - це створення цифрового зображення фізичних об'єктів або атрибутів; в рамках оцифрування не відбувається змін структури інформації, вона просто набуває електронну форму для подальшої обробки в цифровому форматі;

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

соціальна мережа – соціальна структура, утворена індивідами або організаціями, вебсайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів;

хмарні технології – це технології, які надають користувачам Інтернету доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервісу;

цифрова компетентність – здатність використовувати цифрові медіа й електронні освітні ресурси (ЕОР), розуміти та критично оцінювати різні аспекти медіа - цифрових і контенту, а також якості, що вказує на рівень кваліфікації практичного використання ЕОР;

цифрова технологія - сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації;

цифровізація - процес впровадження цифрових технологій у всі сфери суспільного життя.

Інші терміни вживаються у даному Положенні у значеннях, визначених законодавчими актами України.

II РОЗДІЛ. Системотехнічне забезпечення цифрового освітнього простору закладу дошкільної освіти

Цифровий освітній простір закладу дошкільної освіти складають наступні компоненти:

внутрішні: комп'ютери, цифрове діловодство;

зовнішні: ресурси дистанційної освіти, вебсайт закладу освіти, інтернет канали працівників, месенджери, соціальні мережі.

Забезпеченість робочими комп'ютерами

1. Загальна кількість комп'ютерів в закладі освіти - 2, ноутбуків - 3.

Працівники можуть самостійно налаштовувати свої особисті комп'ютери, особливо якщо вони працюють з власних пристроїв.

Загальні настанови та рекомендації щодо налаштувань і доступів до мережі:

1. Пароль і безпека:

Встановіть надійний пароль для вашого комп'ютера, мережевого обладнання та облікових записів.

Регулярно оновлюйте паролі і уникайте використання слабких або очевидних паролів.

Використовуйте двоетапну аутентифікацію, якщо це можливо, для додаткового рівня безпеки.

2. Оновлення програмного забезпечення:

Переконайтеся, що ваша операційна система та інші програми на комп'ютері оновлені до останніх версій.

Включіть автоматичне оновлення, щоб отримувати нові патчі і виправлення безпеки.

Захист від шкідливих програм.

3. Встановіть надійне антивірусне програмне забезпечення та антивірусні програми.

Регулярно скануйте свій комп'ютер на віруси та шкідливе ПЗ.

Уникайте відкриття підозрілих посилань або вкладень в електронних листах.

4. Налаштування мережі:

Встановіть пароль для вашої бездротової мережі Wi-Fi, щоб запобігти несанкціонованому підключенню.

Вимкніть безпроводне підключення (Wi-Fi) або від'єднуйте комп'ютер від мережі, якщо ви не використовуєте Інтернет.

5. Налаштування фаєрволу:

Увімкніть фаєрвол (брандмауер) на комп'ютері для блокування небажаного мережевого трафіку.

Налаштуйте фаїрвол таким чином, щоб дозволити доступ лише до необхідних служб і портів.

6. Керування обліковими записами:

Створюйте окремих користувачів для кожного працівника та надавайте їм відповіді.

Ліцензійне програмне забезпечення

На комп'ютерні програми, які використовуються в закладі освіти, поширюється дія Закону України «Про авторське право і суміжні права», і їх використання можливе лише за умови дотримання вимог цього закону, а також вимог ліцензії, з якою користувач погоджується, установлюючи програму на свій комп'ютер.

Порядок оновлення доступу при звільненні працівника

Для забезпечення цифрової безпеки в закладі дошкільної освіти при звільненні працівника виконуються наступні дії:

1. Працівник має перенести особисті та робочі файли з пристрою, наданого йому в користування, на особисті електронні носії.
2. Працівник має вийти з усіх облікових записів на пристроях, якими він користується в закладі.
3. Працівник, що звільняється, має передати матеріальні цінності (пристрої), надані йому в користування/наявні в кабінеті, завідувачу господарством або уповноваженій особі.
4. Працівник, що звільняється, має видалитись з усіх корпоративних чатів, або дію виконує адміністратор чатів впродовж/не пізніше наступних 5 днів після звільнення працівника.
5. Особа, відповідальна за створення корпоративних акаунтів, має видалити обліковий запис працівника, що звільняється, впродовж/не пізніше наступних 5 днів після звільнення працівника.

Збереження інформації

Для здійснення збереження та захисту даних закладу дошкільної освіти керівник закладу освіти призначає уповноважену ним особу (осіб), відповідальну за інформаційно-технічне забезпечення закладу дошкільної освіти.

До функціональних обов'язків уповноваженої особи (осіб) вноситься запис:

Встановлення, збереження та оновлення паролів на всіх інформаційних та технічних ресурсах освітнього закладу (адмінські паролі (сайт, база даних закладу, платформа для дистанційного навчання), ключі шифрування, паролі до роутера і т.п.).

При зміні технічного обладнання уповноважена особа (особи) контролює технічні роботи, заміну та встановлення паролів.

Веде роз'яснювальну роботу серед учасників освітнього процесу про необхідність цифрової безпеки у закладі.

Робота з паролями

При встановленні паролів уповноважена особа, працівники користуються правилом складних паролів: пароль повинен містити 8 (12) і більше символів: великі та маленькі літери, цифри, спеціальні символи. Пароль має бути без загальнодоступної інформації (ім'я, прізвище, нік, важливі дати, номери телефонів, ППН, адреси і т.п.); для різних інформаційних ресурсів використовуються різні паролі.

Для збереження паролів використовується:

- паперовий варіант – зберігається в сейфі адміністрації закладу;
- менеджер паролів – спеціальна програма, яка надає можливість тримати паролі у безпеці завдяки шифруванню;
- текстовий документ – зберігається документ в архіві під паролем;
- резервне копіювання для кожного способу.

Доступ до інформації та місця збереження паролів має представник адміністрації закладу дошкільної освіти.

Обслуговування комп'ютерів, які використовуються для спільної роботи здійснюється уповноваженою відповідальною особою.

При наявності комп'ютерів для спільної роботи відповідальна особа має сприяти підвищенню безпеки і захисту робочого місця (персональних даних та комп'ютерних пристроїв):

1. Налаштувати захист. Доступ до груп налаштувати через корпоративні акаунти з будь-яких пристроїв.
2. Забезпечити коректне використання мережі Wi-Fi.
3. Створити журнал реєстрації щодо користуванням ПК.

4. Налаштувати сканер безпеки на ПК.
5. Прописати правила користування зовнішніми носіями інформації (флеш, карти пам'яті)
6. Слідкувати за оновленнями: переконатися, що отримуються автоматичні і інсталиувати всі необхідні для організації оновлення.
7. Заборонити інсталиувати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
8. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, або інше корпоративне сховище. Не зберігати дані лише на локальному комп'ютері.
9. Постійно нагадувати (створювати пам'ятки, викладати їх на видне місце) щодо правил безпеки.
10. Створити групи в хмарному середовищі.
11. Налаштувати наступні рівні захисту:
 - фізичний (на фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій);
 - програмно-технічний (на програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності) ;
 - управлінський (на рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки);
 - технологічний (на технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій);
 - рівень користувача (на рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища);
 - мережевий (на мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою);
 - процедурний (на процедурному рівні вживаються заходи, що реалізуються людьми; групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт).

Функціонування загальної мережі ПК в закладі дошкільної освіти

Персональні комп'ютери (ПК) в закладі дошкільної освіти підключено до загальної мережі Інтернету.

Для підключення ПК до мережі укладено договір з інтернет-провайдером GIGABIT, який забезпечує доступ до Інтернету через кабель (*DSL, оптичний волокно або бездротові технології*).

Рівень доступу до мережі встановлюється шляхом налаштування мережевих параметрів на ПК.

На ПК встановлено тип підключення до мережі – провідний Internet та бездротовий Wi-Fi, а також налаштовано доступ до мережі шляхом введення облікових даних (ім'я користувача та пароль).

III РОЗДІЛ. Електронне діловодство закладу дошкільної освіти

Ведення електронного діловодства в закладі освіти здійснюється відповідно до чинного законодавства та регламентується наказами Міністерства освіти і науки України від 08.08.2022 № 707 «Про затвердження Інструкції з ведення ділової документації у закладах загальної середньої освіти в електронній формі», від 25.06.2018 № 676 «Про затвердження Інструкції з діловодства у закладах загальної середньої освіти».

Термін зберігання документів регламентується Переліком типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів (наказ Міністерства юстиції України від 12.04.2012 № 578/5), Переліком відомчих (галузевих) документів.

Ведення та зберігання ділової документації закладу дошкільної освіти в електронній формі, спільна робота з електронними документами, обмін інформацією, як усередині організації, так і в зовнішній її комунікації, здійснюється із застосуванням одного з хмарних

рішень для роботи з документами – *Dropbox, Mega, Microsoft One Drive, Google Drive* на корпоративній платформі *Google, Microsoft 365, Slack, Trello, Asana*, яка схвалена педагогічною радою та якою володіє та централізовано керує заклад дошкільної освіти.

Власником файлів, які зберігаються в хмарному середовищі закладу дошкільної освіти, є заклад дошкільної освіти, а не окремий працівник, який їх створює або додає. Заклад дошкільної освіти є власником всього контенту, що створюється та зберігається в межах платформи, у тому числі, після звільнення окремих працівників, які їх створювали або додавали.

Адміністратором корпоративної платформи (основний обліковий запис із максимальним доступом до платформи закладу освіти) є відповідальна особа, людина/люди, призначена/призначені наказом керівника закладу дошкільної освіти.

Додатковим адміністратором, на випадок відсутності/недоступності основного адміністратора, має бути керівник (вихователь-методист) закладу освіти.

Доступ до файлів надається не тільки працівнику(ам), який(і) їх створюють чи додають, а й співробітникам, які з ними працюють.

Закладом дошкільної освіти забезпечується контроль доступів.

Адміністрація закладу дошкільної освіти надає та блокує доступ до найцінніших файлів.

До документів у хмарному сховищі надаються різні права доступу, які визначають певні можливості (редагування, коментування чи перегляд) та обмеження відповідно до потреб закладу дошкільної освіти.

Забороняється надання повного доступу за посиланням, для унеможливлення попадання посилань у відкритий доступ, що може призвести до безпекових інцидентів. Доступ надається конкретним людям суто із правами, які їм потрібні для виконання робочих завдань.

Керівник закладу дошкільної освіти розробляє чек-лист з відповідними правами доступу різних груп, що надає можливість цим групам мати доступ до спільних файлів, листування і обмежить доступ іншим групам, користувачам.

Крім прав доступу керівник визначає відповідальних за конкретний документ та циклічність його оновлення.

Для забезпечення роботи з електронними документами та своєчасного їх виконання у закладі дошкільної освіти розробляються та затверджуються схеми проходження електронних документів згідно з розпорядчими документами про розподіл обов'язків між адміністрацією закладу, посадовими інструкціями, номенклатурою справ.

Відповідно до цих схем працівникам надається доступ до електронних документів. Наприклад,

1. Прийом відповідальною особою за діловодство вхідних листів через електронну пошту закладу дошкільної освіти, реєстрація у відповідному електронному журналі вхідної документації, завантаження електронного листа до електронної папки у хмарному сховищі.

2. Резолюція та надання директором закладу дошкільної освіти доступу до електронного листа відповідно до повноважень між членами адміністрації.

3. Контроль за виконанням резолюції здійснює директор закладу дошкільної освіти.

4. Проекти наказів, вихідних документів реєструються відповідальним за діловодство у відповідному електронному журналі реєстрації наказів/вихідних документів та завантажуються до електронної папки у хмарному сховищі.

5. Доступ до електронних версій наказів, вихідних документів надається членам адміністрації відповідно до повноважень.

Контроль за виконанням електронних документів здійснює відповідальна особа за діловодство у закладі дошкільної освіти.

Контроль за виконанням електронних документів включає взяття електронних документів на контроль, визначення форм і методів контролю, перевірку своєчасного доведення електронних документів до виконавців, контроль стану виконання, зняття електронних документів з контролю, направлення виконаного електронного документа до справи, облік, узагальнення й аналіз результатів виконання електронних документів, інформування директора про хід та підсумки виконання електронних документів.

Електронні документи передаються до електронного архіву (зберігаються в захищеному хмарному сховищі). Для передачі електронних справ на зберігання до архіву закладу освіти проводиться експертиза цінності документів.

Архівні електронні документи групуються у справи за відповідними електронними

справами.

Для вилучення електронних документів з архіву складається акт про їх знищення.

До персональних даних в системі ІСУО мають доступ директор, вихователь-методист, з обмеженнями – медична сестра та педагоги закладу.

Куратором створюються резервні копії найцінніших файлів для відновлення інформації при втраті оригіналу, з якого було створено резервну копію.

Інформація, яка обробляється в «КУРС: Дошкілля», підпадає під захист Закону України «Про захист персональних даних».

IV РОЗДІЛ. Засоби зовнішньої комунікації закладу дошкільної освіти (електронна пошта закладу дошкільної освіти)

Електронна пошта – це послуга Інтернету, призначена для пересилання комп'ютерними мережами повідомлень (електронних листів) від користувача одному чи групі адресатів.

Електронна пошта для закладу дошкільної освіти є одним із способів комунікації між всіма учасниками освітнього процесу, дозволяє швидко та зручно обмінюватись листами, інформацією, повідомленнями, матеріалами для навчання.

Не використовуються поштові сервіси, електронні поштові скриньки, заборонені на території України (згідно з Указом Президента від 15.05.2017 №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»).

Для формування адреси електронної скриньки під час реєстрації обирається унікальне ім'я, яке буде використовуватися в електронній адресі, встановлюється пароль для облікового запису.

Частота та періодичність зміни паролів для облікових записів закладу дошкільної освіти встановлюється наказом керівника закладу дошкільної освіти (або даним Положенням).

Визначено електронну пошту закладу дошкільної освіти: gra217@i.ua

Визначається відповідальна особа за зміну паролів та налаштування додаткових параметрів облікового запису. Змінений пароль повідомляється керівнику закладу дошкільної освіти (в конверті для збереження в сейфі).

Закладом дошкільної освіти визначається режим використання корпоративних та особистих акантів, встановлюються правила використання поштових скриньок для співробітників.

Особиста електронна пошта використовується працівниками закладу дошкільної освіти для особистого листування.

Корпоративна електронна пошта використовується для внутрішньої комунікації (між працівниками закладу дошкільної освіти), зовнішньої комунікації (з батьками здобувачів освіти, представниками громадськості, установами та організаціями тощо).

Корпоративна пошта забезпечує зручний та організований спосіб комунікації всередині установи.

Закладом дошкільної освіти визначаються правила використання корпоративної електронної пошти, яка передбачає встановлення обов'язкових норм щодо використання, обмежень і конфіденційності інформації, використання зовнішніх поштових сервісів, обмеження відправки конфіденційних даних та використання пошти ЗДО для особистих цілей тощо.

У разі звільнення працівника електронна скринька таких користувачів ліквідується.

Використання спільних облікових записів (одночасно використовуються багатьма працівниками) в закладі освіти може бути доречним, наприклад, для загальних поштових скриньок, які призначені для спільної комунікації або отримання повідомлень від батьків.

Для здійснення адміністрування електронної пошти закладу дошкільної освіти призначається один або кілька адміністраторів із правом доступу до облікових записів адміністраторів (вирішує заклад освіти, в залежності від кількості учасників навчального процесу).

Рекомендовано, призначати 3 адміністраторів (1 – керівник закладу освіти (контроль), 1 – вихователь-методист (контроль), 1 – налаштування доступу до окремих продуктів і сервісів (супровід).

Адміністратор створює корпоративний обліковий запис для кожного учасника закладу освіти та пароль (з урахуванням рекомендацій для створення надійних паролів), який користувач

може змінити на власний (за бажанням).

Адміністратори корпоративної пошти також можуть мати контроль над керуванням обліковими записами, доступом до електронної пошти та іншими аспектами поштової системи. Вони забезпечують правильну роботу та підтримку інфраструктури електронної пошти в закладі дошкільної освіти.

Адміністратори несуть відповідальність за підтримання конфіденційності та безпеки облікових записів кінцевих користувачів і паролів, пов'язаних із цими обліковими записами; використання облікових записів кінцевих користувачів.

Доступ та захист інформації є важливими аспектами роботи з електронною поштою в закладі дошкільної освіти.

Управління доступом передбачає:

1. Створення ідентифікаційних облікових записів для кожного працівника, щоб забезпечити індивідуальний доступ до електронної пошти.

2. Запровадження рівневого доступу на основі потреб та ролей працівників. Наприклад, хто має право на адміністрування системи, хто може мати доступ до конфіденційної інформації тощо.

3. Шифрування:

- використання шифрування для захисту важливої інформації, що передається через електронну пошту. Шифрування допоможе запобігти несанкціонованому доступу до конфіденційної інформації. Рекомендовано встановити TLS (Transport Layer Security) для шифрування передачі даних між поштовим сервером та клієнтськими пристроями.

- двофакторна аутентифікація: активація двофакторної аутентифікації для облікових записів корпоративної пошти забезпечить додатковий захист облікового запису.

4. Антивірусний захист: встановлення надійного антивірусного програмного забезпечення на комп'ютери та сервери, щоб захистити від вірусів, шкідливих програм та інших загроз безпеці. Періодичне оновлення антивірусних баз даних.

5. Створення паролів:

- запровадження політики паролів закладу дошкільної освіти, яка встановлює вимоги щодо довжини, складності та унікальності паролів.

- забезпечення навчання працівників щодо безпеки електронної пошти, включаючи розпізнавання фішингових атак, зловмисних вкладень та інших загроз.

6. Оновлення паролю та регулярна архівація є важливими процедурами для забезпечення безпеки електронної пошти в освітній установі.

Рекомендації щодо процесів оновлення паролю:

- регулярність: оновлення паролів на облікові записи електронної пошти щонайменше раз на 3-6 місяців.

- складність: пароль повинен бути складним і містити комбінацію великих і малих літер, цифр і спеціальних символів (мінімум 8 символів).

- унікальність: використання унікального паролю для кожного облікового запису. Заборона використовувати один і той же пароль для різних сервісів.

7. Необов'язкові додаткові заходи безпеки: використання двофакторної аутентифікації (2FA) для підвищення рівня безпеки облікового запису (може включати використання одноразових паролів, кодів підтвердження через SMS або використання аутентифікаційних додатків).

Зобов'язання користувачів корпоративної електронної пошти закладу дошкільної освіти визначається закладом дошкільної освіти.

Працівники закладу дошкільної освіти зобов'язані використовувати корпоративну електронну пошту при здійсненні своїх посадових обов'язків, зокрема, відправляти та отримувати електронне листування внутрішнім і зовнішнім кореспондентам з використанням адреси робочої пошти.

Працівник закладу дошкільної освіти не має права:

- а) використовувати електронну пошту закладу для цілей, не пов'язаних з виконанням посадових обов'язків в закладі дошкільної освіти;

- б) повідомляти пароль доступу до адреси скриньки іншим особам;

- в) здійснювати масову розсилку листів зовнішнім адресатам, в тому числі листів рекламного характеру;

г) розсилати листи, що містять:

- конфіденційну інформацію, доступ до якої обмежено чинним законодавством, у тому числі містить державну таємницю, матеріали, використання яких порушує права власності;
- недостовірну інформацію, а також інформацію, що ображає честь і гідність осіб, ганьбить ділову репутацію, пропагує ненависть або дискримінацію людей за расовими, етнічними, статевими, релігійними, соціальними ознаками, закликає до протиправних дій;
- матеріали, що містять віруси або інші комп'ютерні коди; файли, програми, призначені для порушення, знищення або обмеження функціональності будь-якого комп'ютерного обладнання.

Відповідальність за зберігання паролів для корпоративних облікових записів покладається на адміністратора, а в разі зміни пароля користувачем – на користувача.

Обов'язок дотримуватись правил користування корпоративною електронною поштою, акантом, наданим закладом дошкільної освіти, вноситься до посадових обов'язків працівника.

V РОЗДІЛ. Засоби зовнішньої комунікації закладу дошкільної освіти (соціальні мережі, месенджери)

Однією із критично значущих складових управлінського процесу у закладі дошкільної освіти є інформування учасників освітнього процесу та громади про свою діяльність на відкритих загальнодоступних ресурсах.

Інформаційна відкритість забезпечується наявністю у закладі дошкільної освіти майданчиків для інформування учасників освітнього процесу, у тому числі у соціальних мережах, месенджерах.

Сторінки освітніх закладів у соціальних мережах мають свої особливості, які зумовлені властивостями електронної комунікації: оперативність розповсюдження інформації; доступність; спрощений пошук цільової аудиторії; легкість налаштування зворотного зв'язку тощо.

В закладі дошкільної освіти мережева комунікація здійснюється в Facebook, YouTube, Padlet дошці.

Керівник закладу дошкільної освіти спільно з педагогічним колективом визначають зміст (про що) і формат (як) буде здійснюватись інформування громадськості про діяльність закладу дошкільної освіти, обговорюють обмеження щодо висвітлення інформації певного змісту.

Керівник закладу дошкільної освіти призначає адміністратора або адміністраторів (за наявності кількості мереж), які несуть відповідальність за оприлюднення достовірної, точної та повної інформації, а також у разі потреби перевіряють правильність та об'єктивність наданої інформації і оновлюють оприлюднену інформацію.

Адміністратор сторінки закладу дошкільної освіти у соціальній мережі дає дозвіл/запрошує приєднатися до спільноти користувачів соцмереж. Окрім того відповідальна особа (адміністратор сторінки) проводить щоденний моніторинг сторінки у соціальних мережах на предмет розміщення на них несанкціонованої інформації; підвищення онлайн культури спілкування учасників освітнього процесу; збереження персональних даних учасників освітнього процесу.

До несанкціонованої інформації можуть відноситися інформаційні матеріали, які вміщують заклики до насильства, розпалювання соціальної та расової ворожнечі, міжнаціональних та релігійних чвар; екстремістські релігійні та політичні ідеї; інформація, заборонена для поширення серед неповнолітніх; інформації рекламно-комерційного характеру та інформації, яка не належить до сфери діяльності освітнього закладу; інші інформаційні матеріали, які заборонені законодавством України.

Мову інформації на сторінці закладу дошкільної освіти в соціальній мережі визначають закони України «Про освіту», «Про забезпечення функціонування української мови як державної», інші закони України та міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег на сторінці освітнього закладу в соціальних мережах не публікується інформація, що може поставити під загрозу особисте життя особи, життя членів її сім'ї та інших осіб; обмежується доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі; здійснюються налаштування, які найбільше

захищають додаткові відомості про власника аканта, зокрема, не зазначається геолокація (місце розташування освітнього закладу); здійснюється періодичний перегляд списку «друзів» у соціальній мережі (якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу); не використовуються соціальні мережі та пошукові системи (у т.ч. із застосуванням сервісів VPN), доступ до яких обмежено відповідно до Указу Президента України «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

Керівник закладу дошкільної освіти відповідає за визначення завдань, забезпечення та контроль за діяльністю відповідальної особи з питань опрацювання, оприлюднення публічної інформації, передбаченої чинним законодавством.

Для будь-яких контактів чи комунікації між учасниками освітнього процесу закладу дошкільної освіти використовуються спільноти в месенджері.

В закладі дошкільної освіти таким засобом комунікації виступають Telegram-спільноти, Viber-спільноти.

Спільноти, сформовані для комунікації та різного роду інформування учасників освітнього процесу, класифікуються за призначенням: для інформування учасників освітнього процесу про новини закладу дошкільної освіти; для спілкування педагогічних працівників з адміністрацією; для обміну інформацією між педагогами та батьками та інші.

Створюються відкриті спільноти – приєднатись може будь-хто; закриті – призначені для обмеженої кількості учасників, яких запрошує адміністратор.

Керівник закладу дошкільної освіти призначає відповідального адміністратора чи декількох осіб для ведення загальносадової спільноти.

Для всіх інших спільнот за потребою адміністратором може виступати той, хто створює спільноту.

Адміністратор спільноти визначає її правила, в тому числі дозволяє або забороняє учасникам відправляти повідомлення у спільноту.

Спілкування може бути одностороннім (повідомлення пише лише адміністратор, а учасники можуть лише читати, ставити позначки та пересилати їх) або двостороннім (учасники спільноти також можуть надсилати повідомлення).

Адміністратор може змінювати правила спільноти відповідно до ситуації.

В закладі дошкільної освіти обговорюються та приймаються загальні підходи щодо використання месенджерів для функціонування спільнот, зокрема, визначаються обмеження щодо розміщення в спільноті певного контенту.

Інформація, розміщена в спільноті, доступна для всіх його учасників незалежно від того, коли вони приєдналися. Вся історія спілкування зберігається в чаті.

В закладі дошкільної освіти встановлюються чіткі правила щодо спілкування в чатах.

Загальні правила щодо спілкування в чатах обговорюються на засіданнях колегіального органу управління закладом освіти (педради), додаються до правил поведінки (внутрішнього розпорядку), прийнятих в закладі дошкільної освіти.

Правила спілкування в чатах:

- Поважайте чужі часові рамки, бережіть особистий час. Встановіть та дотримуйтесь часових обмежень для надсилання повідомлень (наприклад, не писати у чат після 20:00).

- Дотримуйтесь контексту та тематики групи. Не засмічуйте групові чати зайвою, неактуальною інформацією. Пам'ятайте про мету спілкування, чітко розумійте, для чого ви щось говорите, наскільки конструктивним і доречним це буде.

- Не поширюйте неперевірену інформацію.

- Турбуйтеся про співрозмовників – передавайте інформацію повно, але, водночас, лаконічно.

- Перевіряйте корисність повідомлення: під час відправлення на цілу групу воно повинно стосуватися кожного члена чату. Інакше варто скористатись чатом 1-1. Уважно ставтеся до повідомлень у спільному чаті: іноді ми поспішаємо із відповіддю і перепитуємо про те, що в чаті вже написали.

- Не ображайте учасників чату, дотримуйтесь етики спілкування, принципів толерантності, відкритості, свободи думки, совісті і переконань,

- Дотримуйтесь правил мережевого етикету: використовуйте зрозумілу мову, транслюйте

правильний тон і настрій, пишіть грамотно (помилки у словах тощо – значно знижують якість розмови та ускладнюють взаєморозуміння), не переобтяжуйте повідомлення текстом, стікерами й емодзі, уникайте потенційно образливих слів та висловів, а також того, що у письмовій формі може бути трактовано двозначно, неправильно.

- Не використовуйте нецензурну лексику, саморекламу, спам.
- Уникайте переходу на особистості та оціночних суджень, не допускайте будь-яких форм дискримінації.
- Дотримуйтесь правила емоційної рівноваги. Не пишіть в чат під час емоційного навантаження, стресу. Основа екологічного спілкування – це доброзичливий тон та взаємна підтримка.
- За порушення правил вводиться обмеження: адміністратор може тимчасово видаляти учасника або відправляти у бан на певний час.
- Будьте чесними та уважними – лише тоді спілкування залишатиметься щирим та довірливим.

Правила закріплюються у чаті за допомогою відповідної функції закріплення повідомлень.

Презентація закладу дошкільної освіти в соцмережах, здійснення спілкування його працівників в месенджерах має бути коректним, професійним, етичним. Важливо сформувати у працівників закладу дошкільної освіти розуміння ризиків втрати онлайн-репутації – власної та закладу дошкільної освіти.

Між приватним та професійним життям педагогів, зокрема, й у цифровому середовищі, важливо встановити чітку межу.

Для будь-яких контактів між співробітниками закладу дошкільної освіти та батьками в закладі освіти використовується корпоративна (офіційна) електронна пошта.

Для безпеки педагогів варто створити окремий обліковий запис або окремого користувача, якщо пристроєм – комп'ютером, ноутбуком, планшетом – вдома чи на роботі користується кілька користувачів, розмежувати власні електронні скриньки для особистого користування та для робочих питань.

Комунікаційна політика закладу дошкільної освіти забороняє (*обмежує*) будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу.

На випадок проведення відеоконференцій або занять у віддаленому режимі, закладом дошкільної освіти установлюються чіткі приписи як для співробітників, так і для здобувачів освіти (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч).

VI РОЗДІЛ. Особливості організації освітнього процесу.

Організація освітнього процесу в закладі відбувається відповідно до нормативних документів Міністерства освіти і науки України, згідно зі статутом закладу дошкільної освіти, з урахуванням стану функціонування освітнього середовища закладу дошкільної освіти, його матеріально-технічних, системотехнічних, кадрових можливостей, стратегічних перспектив розвитку закладу дошкільної освіти.

Забезпечення цифрової безпеки необхідно в умовах організації освітнього процесу за дистанційною формою та/або з використанням технологій дистанційного навчання.

Для забезпечення діяльності закладу дошкільної освіти в умовах режиму дистанційного навчання в закладі освіти прийнято Стратегію (*Положення*) дистанційного навчання, яким узгоджено правила та алгоритми взаємодій усіх учасників освітнього процесу для виконання освітніх програм закладу в даному форматі надання освітніх послуг.

Визначено перелік сервісів для проведення відеоконференцій та онлайн-зустрічей (*ZOOM, GoogleMeet*) в закладі дошкільної освіти для здобувачів освіти різних вікових категорій.

З метою захисту персональних даних під час дистанційного навчання забезпечується дотримання вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

В закладі освіти використовується захищена та надійна мережа: використовуються послуги офіційного інтернет-провайдера Флагман.

В разі використання педагогами та батьками вихованців під час дистанційного навчання особистих домашніх пристроїв, які зазвичай не охоплюються мережевим захистом, проводиться робота щодо ознайомлення педагогів та батьків з необхідністю перевірки надійності інтернет-провайдера, а також системна робота з навчання всіх учасників освітнього процесу правилам поведінки в інтернеті для забезпечення безпеки учасників освітнього процесу, зокрема, шляхом системної роботи з розвитку цифрової грамотності; вивченню функціоналу програмних засобів, визначених для організації освітнього процесу (формування запрошення на відеоконференцію, блокування чату, надання різного роду доступів: до демонстрації екрану, спільного використання онлайн-документів, онлайн-дошки під час відеоконференції тощо); надання рекомендацій педагогам, батькам вихованців щодо встановлення на всіх пристроях брандмауера та антивірусних програм, батькам – за необхідності – програм фільтрації, блокування або відстеження, використання контент-фільтрів (системи батьківського контролю) і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в інтернеті.

Організовано ознайомлення учасників освітнього процесу з політикою закладу дошкільної освіти, що регулює використання інформаційних технологій (сервісів, ресурсів) різними учасниками освітнього процесу.

Закладом дошкільної освіти проводяться заходи щодо дотримання авторського права.

Відповідно до Положення про академічну доброчесність в закладі дошкільної освіти забезпечується дотримання академічної доброчесності всіма учасниками освітнього процесу.

Спільно з батьками вихованців в закладі дошкільної освіти приймається рішення щодо умов проведення відеозйомки навчальних занять, публікації відеоматеріалів або творчих робіт дітей у мережі Інтернет (на сайті закладу дошкільної освіти, на сторінках соцмереж).

В закладі дошкільної освіти визначено порядок реагування працівників на інциденти, пов'язані з безпекою дітей, зокрема в цифровому середовищі:

- негайне інформування відповідальної особи або керівника закладу дошкільної освіти про інцидент, пов'язаний з безпекою дітей, що виник в цифровому середовищі, для прийняття рішення щодо подальших дій: інформування батьків дитини, відповідних служб та установ правопорядку про встановлені порушення прав дитини;

- збереження (фіксація) ознак інциденту, у тому числі на матеріальних носіях;
- забезпечення захисту інформаційних ресурсів закладу дошкільної освіти;
- проведення, за потреби, відповідної профілактичної роботи з вихованцями та батьками.

Визначено відповідальну особу за розгляд інцидентів, пов'язаних з онлайновою безпекою, та організацію відповідної просвітницької роботи.

Використання технічних засобів навчання та мобільних пристроїв (ноутбуків, планшетів, смартфонів) під час дистанційного навчання є базовою умовою для організації освітнього процесу засобами цифрових технологій. Закладом дошкільної освіти проводиться робота з інформування учасників освітнього процесу щодо забезпечення безпеки пристроїв під час навчання.

Використання мобільних пристроїв в освітніх цілях під час очного навчання допомагає урізноманітнити заняття, сприяти навчанню вихованців, зокрема розвивати в них медіаграмотність.

Умови та правила використання мобільних технологій та інших електронних пристроїв в закладі дошкільної освіти обговорюються та приймаються колективно, вносяться до правил поведінки в закладі дошкільної освіти.

Про дотримання цих правил інформуються всі учасники освітнього процесу.

VII РОЗДІЛ. Проведення заходів просвітницького характеру

З метою дотримання права дитини на безпеку та захист, яке є базовим та поширюється на її життєдіяльність як офлайн, так і онлайн, з урахуванням пріоритетного значення цифрових компетентностей для ефективного навчання та успішного життя людини в сучасному світі, формування навичок безпечної поведінки дитини в цифровому середовищі з раннього віку в закладі дошкільної освіти проводиться система профілактичних заходів просвітницького характеру з підвищення рівня знань в області інформаційно-комунікативних технологій, з питань безпечної поведінки в інтернеті, медіаграмотності.

Для організації роботи з учасниками освітнього процесу в закладі дошкільної освіти

здійснюються наступні кроки:

1. Визначаємо складові формування навичок безпечної поведінки в цифровому середовищі, зокрема, права людей (зокрема, права в цифровому середовищі); електронна участь (в ухваленні рішень); збереження здоров'я під час роботи з цифровими пристроями; механізми захисту прав, що порушуються в інтернеті, а також способи отримати допомогу.

2. Визначаємо коло осіб, які причетні до цифрової комунікації учасників освітнього процесу: педагоги, здобувачі освіти (вихованці), батьки, інші особи, з якими може бути налагоджено (можуть бути учасниками) організацію таких заходів.

3. Плануємо та організовуємо профілактичні заходи з метою підвищення обізнаності педагогів, батьків та їхніх дітей.

4. У разі виявлення, що дитина стала жертвою будь-яких проявів насильства, експлуатації, вербування або маніпуляцій у цифровому просторі, інформуємо керівника закладу дошкільної освіти, який приймає рішення про звернення до Національної поліції України та надсилання повідомлення про правопорушення до департаменту кіберполіції Національної поліції України. Доводимо до постраждалого інформацію про можливість отримання психологічної допомоги та підтримки.

Керівник закладу призначає відповідальну особу (осіб) з питання щодо просвіти учасників освітнього процесу.

Проведення заходів відповідно до Програми просвітницької роботи може здійснюватись відповідальною особою, призначеною керівником закладу освіти педагогом.

До Програми просвітницької роботи можуть вноситись зміни з урахуванням динамічного розвитку цифрових технологій та відповідно до актуальних потреб учасників освітнього процесу.

Орієнтовна Програма просвітницької роботи з учасниками освітнього процесу.

I Просвітницькі заходи з педагогами як суб'єктами гарантування цифрової безпеки.

Просвітницькі заходи з працівниками закладу дошкільної освіти спрямовуються на підвищення рівня цифрової компетентності.

Попередньо визначається рівень спроможності педагогів працювати у цифровому середовищі з урахуванням того, що педагогам необхідно:

- володіти інформацією щодо можливостей цифрових технологій;
- формувати вміння вибрати ту технологію, цифрові інструменти, які відповідають його педагогічній діяльності;
- бути тренером (ведучим) у процесі формування навичок комунікації дітей, батьків з питань поведінки у цифровому просторі;
- вміти оцінювати отриману інформацію з точки зору реалізації в професійній діяльності та визначати особисті потреби у підвищенні кваліфікації в даній сфері;
- вміти виступати посередником під час соціальної активності між всіма учасниками освітнього процесу.

Для забезпечення правильного формування цифрової компетентності педагога він повинен мати:

- навички володіння методами та прийомами інформаційної діяльності;
- сформовані професійні навички та уміння, що забезпечуються використанням цифрових технологій у роботі;
- можливість безпосереднього використання знань, умінь і навичок з використання цифрових технологій у професійній сфері;
- мотивацію до удосконалення знань та вмінь використання цифрових технологій в професійній діяльності та житті;
- можливість забезпечення розвитку професійних якостей працівника, підвищення рівня освітніх послуг за допомогою цифрових технологій.

№	Просвітницькі заходи	Примітки
---	----------------------	----------

1.	Для підвищення рівня обізнаності освітян щодо небезпек в мережі Інтернет: організація семінарів та навчальних курсів для освітян з питань цифрової безпеки, які охоплюють теми захисту персональних даних, безпеки паролів, використання безпечних мереж Wi-Fi, виявлення фішингових атак та інші аспекти цифрової безпеки.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
2.	Для здобуття освітянами цифрової освіти з використанням інформаційних ресурсів: підготовка та розповсюдження матеріалів: пам'яток, брошур або інші матеріали з цифровою безпекою, які освітяни можуть використовувати в своїй роботі з учнями та вихованцями; надання учителям та вихователям як суб'єктам гарантування цифрової безпеки доступу до актуальних інформаційних ресурсів та рекомендацій з цифрової безпеки.	Згідно з ключовими положеннями, передбаченими Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
3.	Для обміну досвідом освітян як суб'єктів гарантування цифрової безпеки: створення форуму або онлайн-спільноти, де працівники закладу освіти зможуть обмінюватися досвідом та кращими практиками з цифрової безпеки; ділитися успішними стратегіями використання цифрових інструментів в професійній діяльності.	
4	Для підвищення рівня медіакультури та медіаграмотності: проведення тренінгів та майстер-класів для освітян з використанням сучасних інструментів для створення пізнавальних ігор та інтерактивних ресурсів; створення/перегляд/обговорення методики використання спеціальних мультиплікаційних відеороликів, які наголошують на безпеці в Інтернеті для дошкільнят та молодших школярів; встановлення партнерства з місцевими медійними організаціями або журналістами для проведення майстер-класів, тренінгів або стажування для учнів, де вони зможуть поглибити свої знання з медіа грамотності.	Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 № 685/2021
5	Для підвищення рівня інфомедійної культури педагогів в соціальних мережах: сприяння участі педагогів у вебінарах, прослуховуванні навчальних курсів, тренінгах, інтерактивних формах навчання, які формують складові інфомедійної культури дорослого особисто та як тренера для дітей у подальшому.	

6	Для підвищення практичних вмінь педагогів щодо побудови партнерських взаємовідносин між закладом освіти і родиною з питань безпечної поведінки дитини у цифровому середовищі: проведення тренінгів для формування навичок комунікації з батьками з питань поведінки у цифровому просторі; формування навичок стимулювання у батьків соціальної активності щодо обміну досвідом з питань формування безпечної поведінки дітей у цифровому просторі.	МОНУ (№1/9-128 від 10.03.2021 «Щодо необхідності проведення додаткових профілактичних заходів в середовищі дітей та підвищення обізнаності батьків»).
---	--	---

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з вихованцями:

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки можуть включати формування цифрових компетентностей для навчання та життя, ознайомлення з основами кібербезпеки, правилами безпечної роботи в Інтернеті, інформування про коректне використання антивірусного програмного забезпечення та інших інструментів захисту від кібератак.

1. Визначення рівня умінь дітей дотримуватись правил безпечної поведінки в інтернеті:

- *не розповсюджує особисті дані (адресу проживання, місце навчання, номер мобільного телефону, інформацію про батьків) в Інтернеті;*
- *якщо трапилась неприємна ситуація – звертається по допомогу до дорослих, кому дитина довіряє (батьки, старший брат чи старша сестра, вихователь у садочку);*
- *не зустрічається (не прагне зустрітись) з тими, кого ми знаємо тільки онлайн;*
- *не відповідає на повідомлення, які є неприємними, повідомляє про них дорослому;*
- *розповідає (готовий розповісти) батькам, якщо хтось надсилає чи говорить неприємні слова;*
- *ні з ким не ділиться (знає правило) своїм паролем до гаджету чи додатку, доступом до власного профілю в соцмережі тощо;*
- *перед завантаженням нового додатку запитує (запитає) дозволу у батьків (діти 4-6(7) років).*

2. Відповідно до отриманих результатів щодо рівня умінь дітей дотримуватись правил безпечної поведінки в цифровому просторі визначаються напрямки/відповідні заходи просвітницького характеру з вихованцями.